ESERCIZI SVOLTI SUI POLINOMI

Giovanni Ferranti <gyofer@yahoo.it>

a) x^4+x+1 in $Z_2[x]$ l'equazione data non ha radici perchè gli elementi in Z_2 sono $\{0,1\}$ perciò non si annulla MAI!! Potrebbe essere prodotto di 2 polinomi di 2° grado, che si suppongono monici.: Quali sono?

$x^2+a_1x+a_0$ per a_1 e a_0 Le due possibili scelte (o 0 o 1 in Z_2).
I quattro polinomi MONICI possibili sono:
x^2
x^2+x
x^2+1
x^2+x+1
x^4 si annulla da 0 e non va, perchè x^4+x+1 non deve avere radici. Idem con x^2+x che non va. x^2+1 implicherebbe che x^4+x+1 ha una radice perchè se x=1 si ha 1+1=2=0 in Z_2 e non va. L'unico che va bene è x^2+x+1 che può essere solo moltiplicato per se stesso.
(x^2+x+1)(x^2+x+1)= $x^4+x^3+x^2+x^3+x^2+x+x^2+x+1=x^4+x^2+1$ (che è diverso da quello iniziale) (si cercano quelle con coefficiente 2 perchè 2=0)
Quindi x^4+x+1 è IRRIDUCIBILE in Z_2.
b) x^4+3x+5 in $Z[x]$
c) $3x^4+2x^3+4x^2+5x+1$ in $Z[x]$

b) si valuta il polinomio in $Z_2[x]$, se è irriducibile lo è anche in $Z[x]$.
In $Z_2[x]$ è x^4+x+1 che è irriducibile (lo si è visto nell'es. a)).
c) Stesso trucco: il polinomio in $Z_2[x]$ diventa:
x^4+x+1 (perchè i termini con coefficienti=n2 se ne vanno perchè 2=0 in Z_2 perciò i coefficienti pari sono in realtà 0 in Z_2, quelli dispari sono 1) perciò è irriducibile in $Z_2[x]$ $\Rightarrow$lo è anche in $Z[x]$.
Bisogna sempre trovare una s tale che in $Z_s[x]$ quel polinomio è irriducibile per sapere se lo è in $Z[x]$.
Bisogna aver fortuna (trovare l'intero tale che quel polinomio mod. quell'intero è irriducibile).
d) $2x^5-3x^4+15x^2-3x+30$ $\leftarrow$ Eisenstein in Z_3 irriducibile. in $Z[x]$.
e) $x^5+4x^4+2x^3+3x^2-x+5$ in $Z[x]$. (il polinomio e) non vuole Eisenstein)

e) si può fare quozientando $Z_2[x]$ dove è RIDUCIBILE, ma non ci aiuta.
$Z_3[x]$ dove il polinomio è $x^5+x^4+2x^3+2x+2=\overline{f}(x)$ Le radici? 0,1,2 niente da fare.
Non ha radici. Deve essere prodotto di polinomi di grado ≥ 2 cioè $(x^2+.....)(x^3+......)$
x^2+x
x^2+x+1
x^2+x+2
x^2+2x
x^2+2x+1
x^2+2x+2
x^2+1
x^2+2
x^2
sono i possibili (x^2+....)

si scartano quelle che hanno una radice: x^2, x^2+x, x^2+2x, x^2+2 (perchè si ha radice 1),
x^2+x+1.
Rimangono 4 polinomi:
$[x^2+x+2$
x^2+2x+1 si ha radice 2 e si toglie
$[x^2+2x+2$
$[x^2+1$
Rimangono 3 polinomi.
Prendo $Z_3[x] / x^2+1$ la classe di $\overline{f}$ deve essere = 0

$Z_3[x] / x^2+1 = \{a\alpha + b | \alpha^2 + 1 = 0\}$ devo tradurre $\overline{f}$ in termine di α $\alpha^2 = -1$

$[\alpha^5 + \alpha^4 + 2\alpha^3 + 2\alpha + 2]_{\alpha^2+1}$ ma $\alpha^2 = -1$ e perciò si ha:

$\alpha + 1 - \cancel{2\alpha} + \cancel{2\alpha} + 2 = \alpha + 3 = \alpha$ in Z_3 $\alpha \neq 0$
perciò il polinomio dato non è 0 e non è divisibile per x^2+1.
Si prosegue e si scopre che il polinomio è irriducibile.